Future of Trust

Mirco Rohr
Director Solutions Consulting EMEA

13th October 2025

Why Mastercard

Mastercard has been applying our cybersecurity principles to secure our global payments network for the past 50 years

- We Securely Store Over 18 Petabytes of Sensitive Data
- Secure Data & Transactions for 2.7 Billion Cards Annually
- Mitigate 3.2 Million Phishing Attempts on Our Network Annually
- Detect & Defeat 200 Attacks on our Network Every Minute of Every Day

We are now bringing our decades of expertise and those same high standards of quality, reliability, security, and privacy to the broader ecosystem

The challenge of third-party cyber risk

Manual risk assessments are slow, inconsistent, and resource-intensive. Organizations lack the resources to proactively monitor and assess all the vendors holding their critical data

41B

connected devices in 2023 with an 18% higher growth rate than 2022[1]

59%

of organizations have experienced a data breach caused by a third party[2]

$1.4M

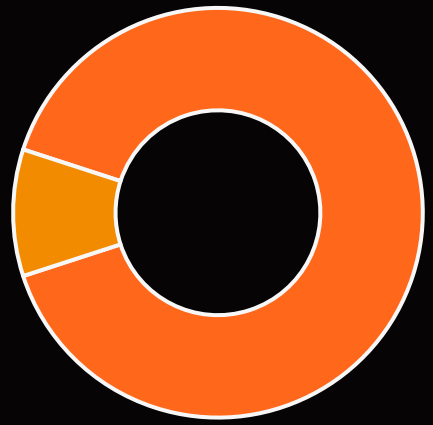
Is the average cost of a multi-party data breach[3]

1. Frost & Sullivan. Top growth opportunities for iot in 2023. march, 2023.
2. The 2022 data risk in the third-party ecosystem study. PONEMON INSTITUTE. 2022.
3. Cyentia Institute: riipples across the attack surface. oct 2023.

The Legacy Approach to Third-Party Risk Management

Questionnaire-driven: vast majority of time + resources spent on administering questionnaire requests

10%
Risk Mitigation



90%
Administrative, manual efforts

Impact

- **Manual, unscalable processes**
- **Exposure to additional risk**
- **Vendor fatigue, pushback, and chasing**
- **Elongated purchasing processes**

Why?

- **Time-consuming** bespoke questionnaire requests
- **Inability to leverage** existing vendor documentation
- **Lack of headcount** and resources

Examining Data Breaches Around the World

14,413

breach events since 2012

1,454

destructive ransomware events since 2016

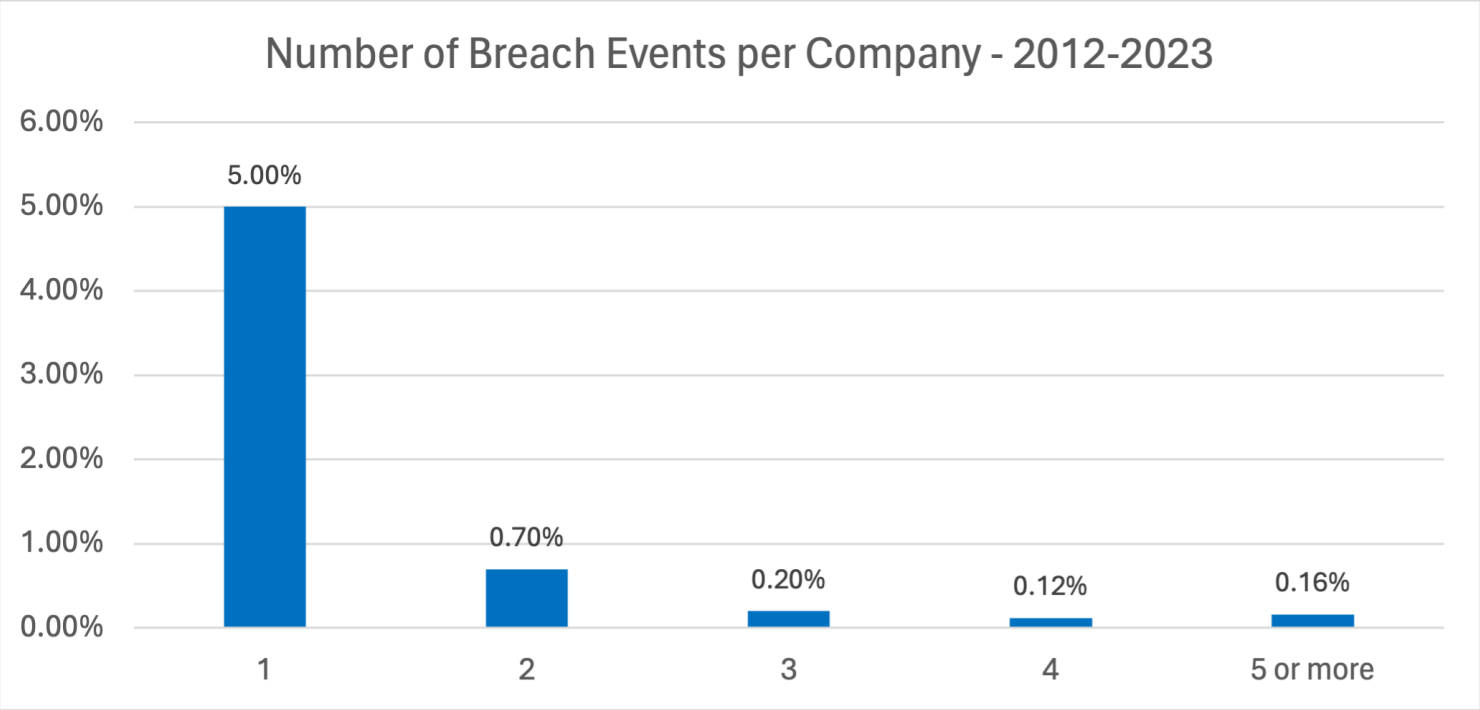
6.2%

of companies have publicly reported a data breach since 2012

1.3%

of companies have publicly reported a destructive ransomware event since 2016

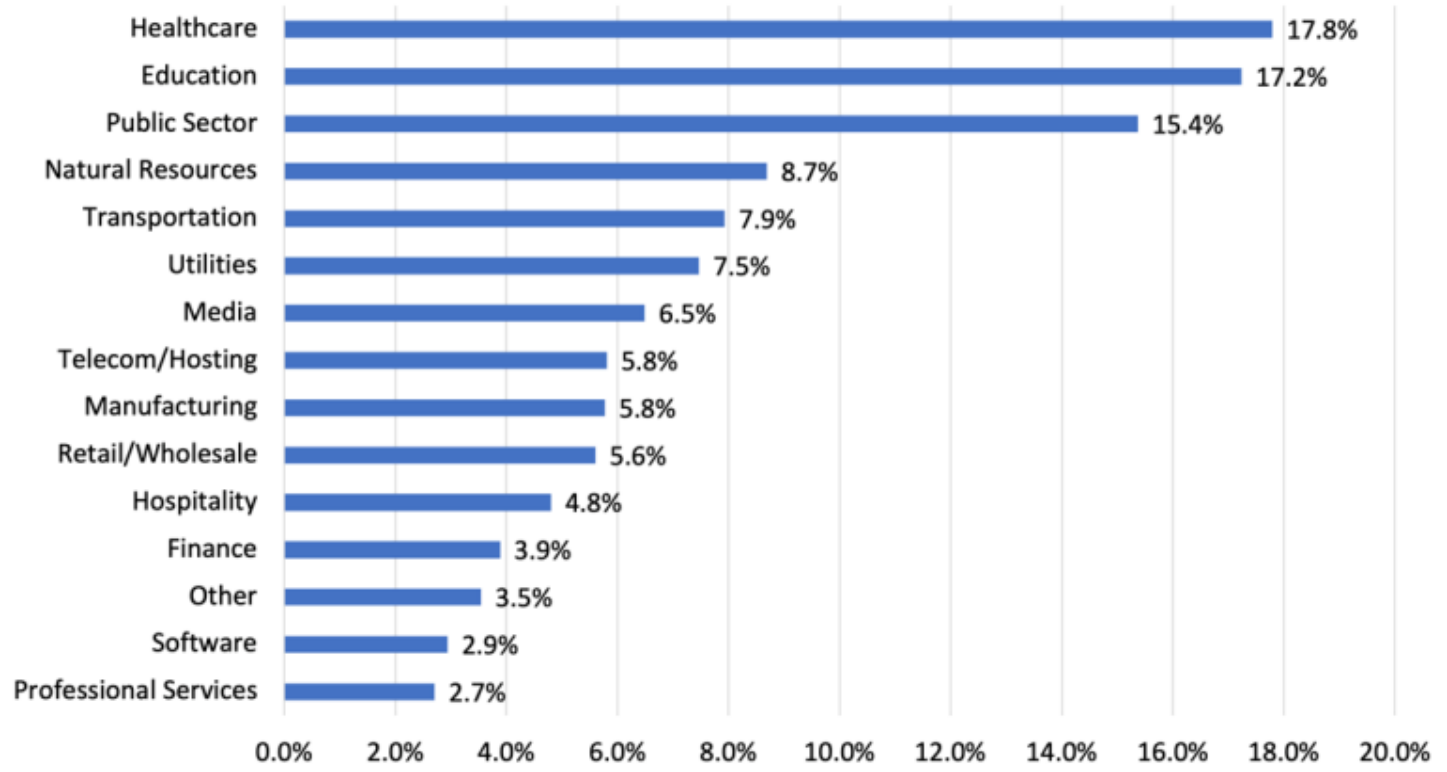
Companies with one breach event most likely population to report another



20%

of breached companies will have another breach within 12 years

The Good News for the Hospitality Industry



4.8%

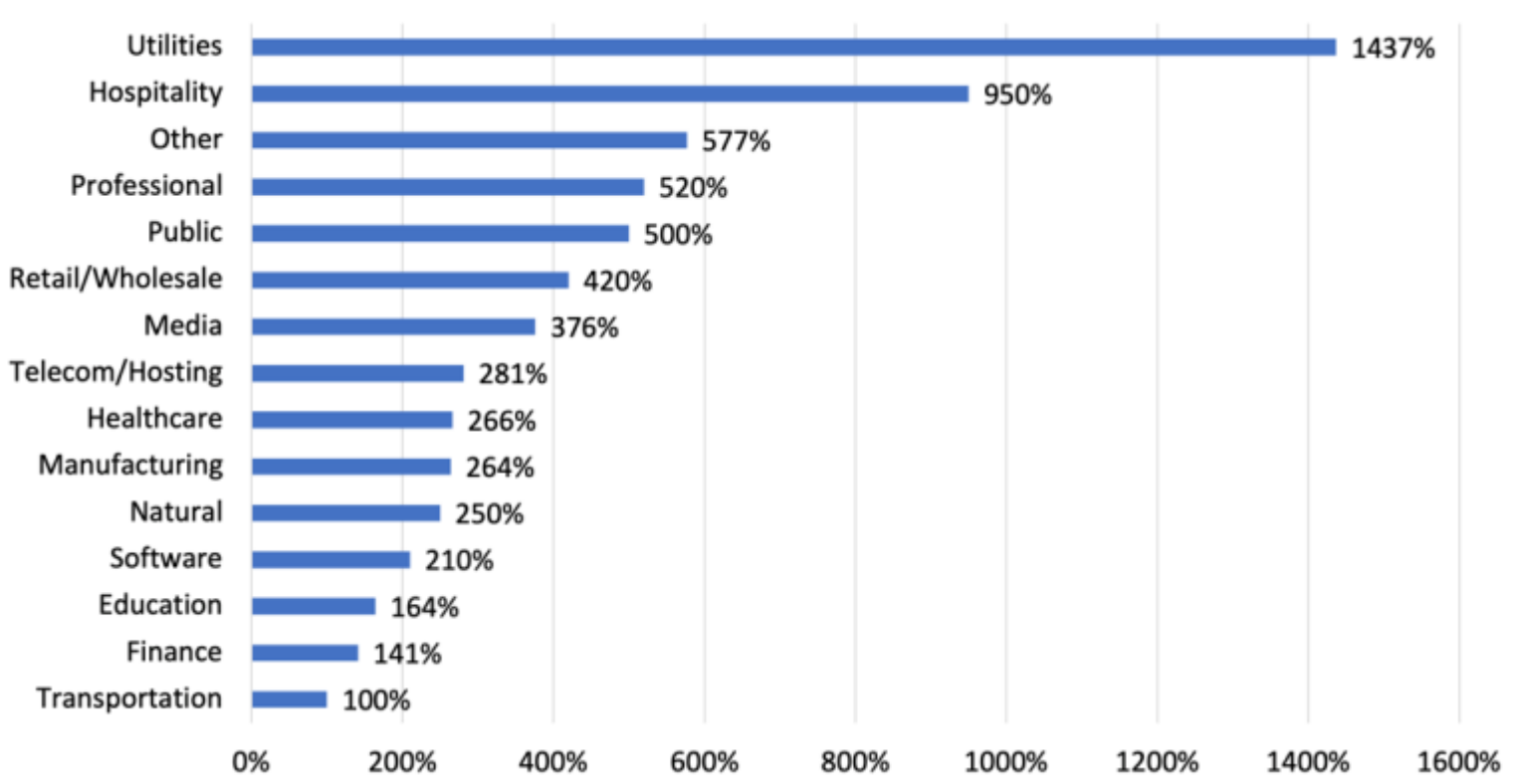
Only 4.8% of hospitality organizations have publicly reported a breach event since 2012

The Bad News for the Hospitality Industry

9.5X

The hospitality industry has reported 9.5 times more breach events since 2012

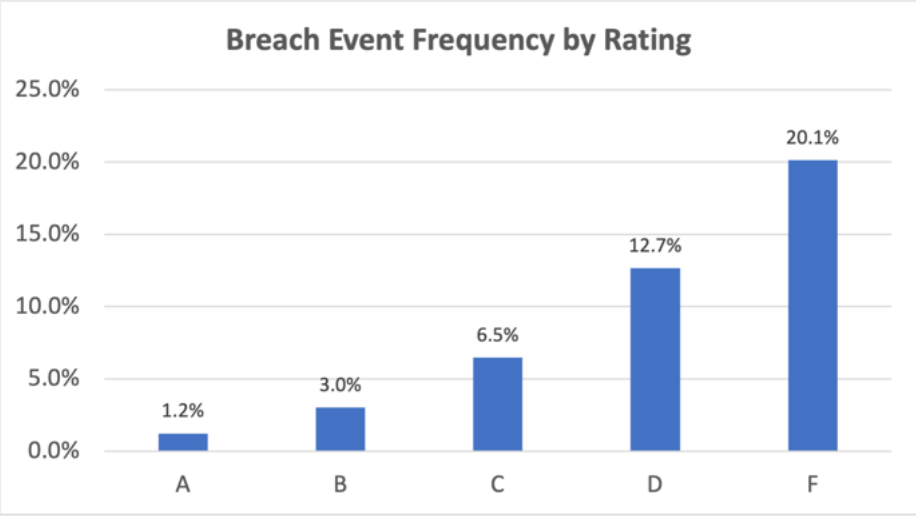
The Bad News for the Hospitality Industry

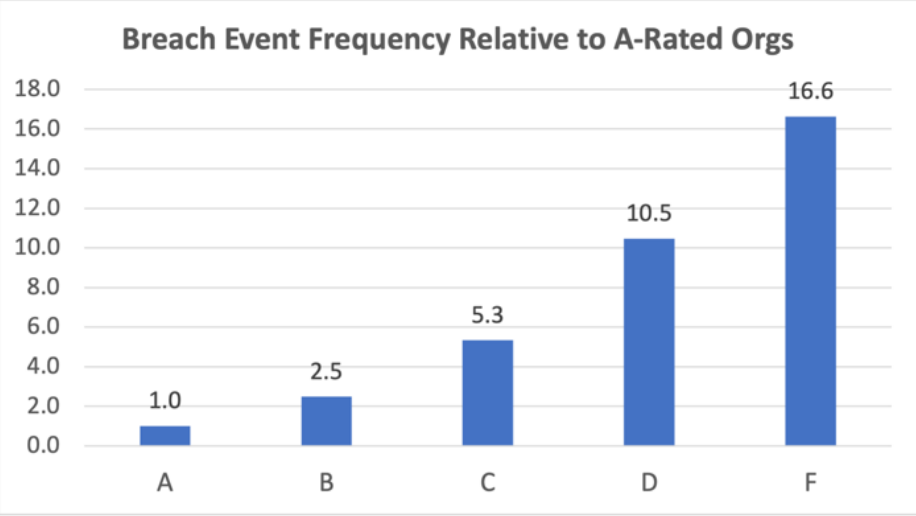


950%

The hospitality industry has experienced the second highest rate in data breaches across all of the industries we studied since 2012

Poor cybersecurity hygiene = 13x higher breach event frequency





	Average Issue Count		
	Breach Victim	**General Population**	**Difference**
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	35.5	4.1	8.7x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	15.0	1.7	8.8x higher
Application Security Issues Missing common security practices in applications that collect sensitive data	17.8	2.6	6.8x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	43.4	6	7.2x higher
Email Security Issues Security issues in active email servers and domains that increase susceptibility to phishing and data theft	27.2	2.8	9.6x higher
System Reputation Issues Number of systems exhibiting malicious activity such as communicating with botnet controllers, block-listed for attempting to compromise other systems or spamming	8.1	0.3	27x higher

Where do we go from here with TPRM?

Do I really need to do more in TPRM?

80%

Report that inaccurate questionnaire answers are not uncommon

5%

Of “A” rated vendors still experience a breach

26%

Manage at least 250 vendors, double from 2020

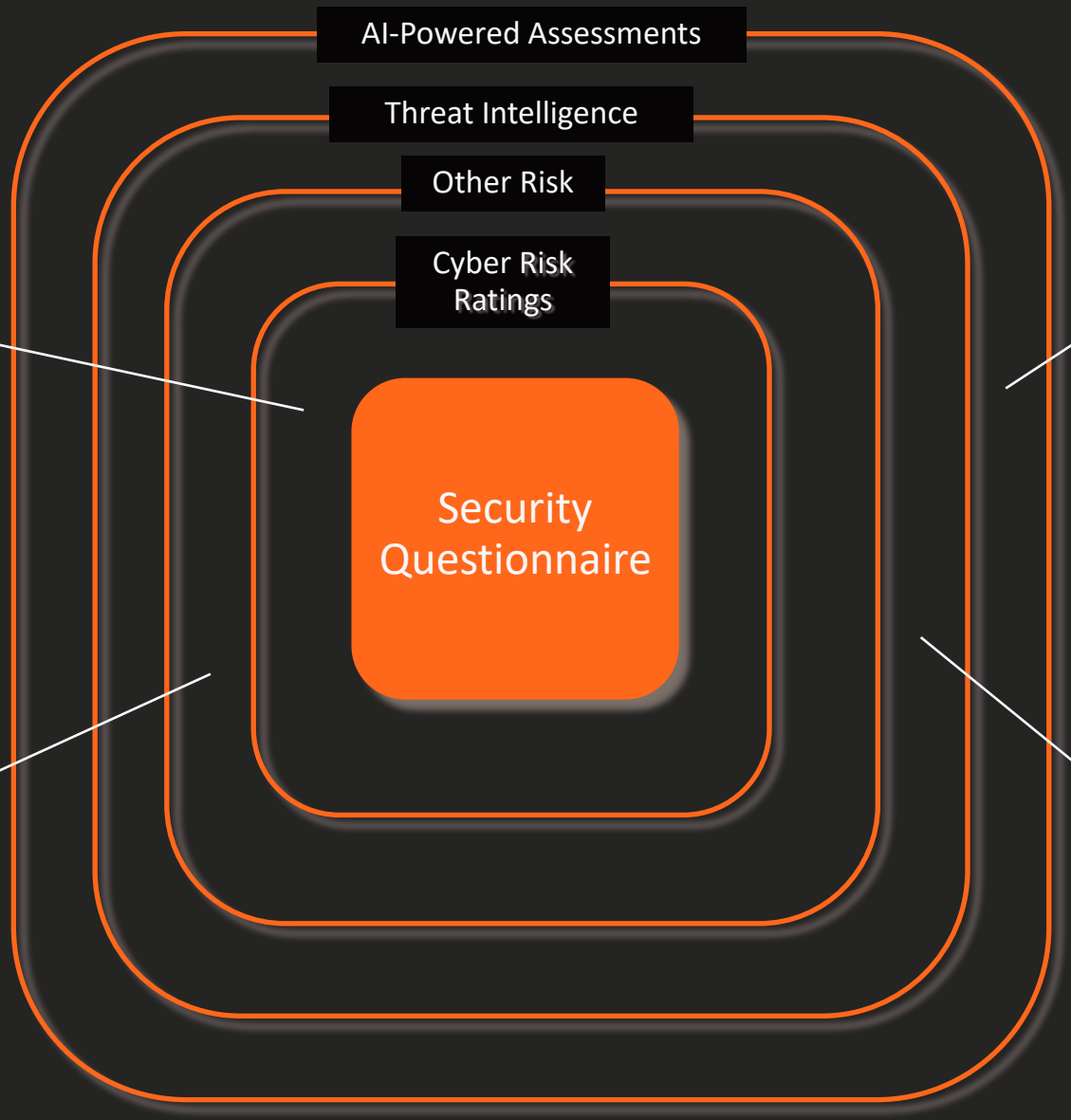
43%

Claim their TPRM program is adequately staffed

The 2024 State of Third-Party Risk Management

https://www.riskrecon.com/state-of-third-party-risk-management-2024

Building a Better TPRM program



Cyber Risk Ratings

- What does the third-party's external cyber posture look like?
- Does it match what the questionnaire is telling me?
- High risk CVEs?
- Has a breach occurred or is it likely to?

Other Risk

- Does the third-party have financial problems?
- Are they located in an area with geo-political issues?

AI-Powered Assessments

- With all this data, are there any connections?
- How can I do more without needing more resources?
- What do I need to care about right now?

Threat Intelligence

- Are there credentials exposed?
- Information for sale on the dark web?
- What is happening right now?

One trusted approach

MASTERCARD CYBERSECURITY

Assess
risk exposure

Understanding multi-dimensional risks, vulnerabilities, and threats at the speed of business

Protect
against attacks

Addressing risks using unique intelligence and multi-layered cloud-based defense technology

Organize
ecosystem trust

Orchestrating continuous improvement of global cyber security and risk

Assess risk exposure

Helping organizations gain greater risk visibility within their business, amongst their third-parties, and deeper into their supply chain.

HOW?

By understanding multi-dimensional risks, vulnerabilities, and threats at the speed of business.

WHY?

With increased supply chain connections, organizations need steadfast ability to manage and assess risk at scale.

Our AI and machine learning technologies and solutions empower businesses to continuously measure and monitor high volume risk, overtime – enabling better standardization and benchmarking.

Solution offerings

Cyber Quant

Cyber Front

Cyber Insights

Cyber Secure

Cyber Crisis Exercise

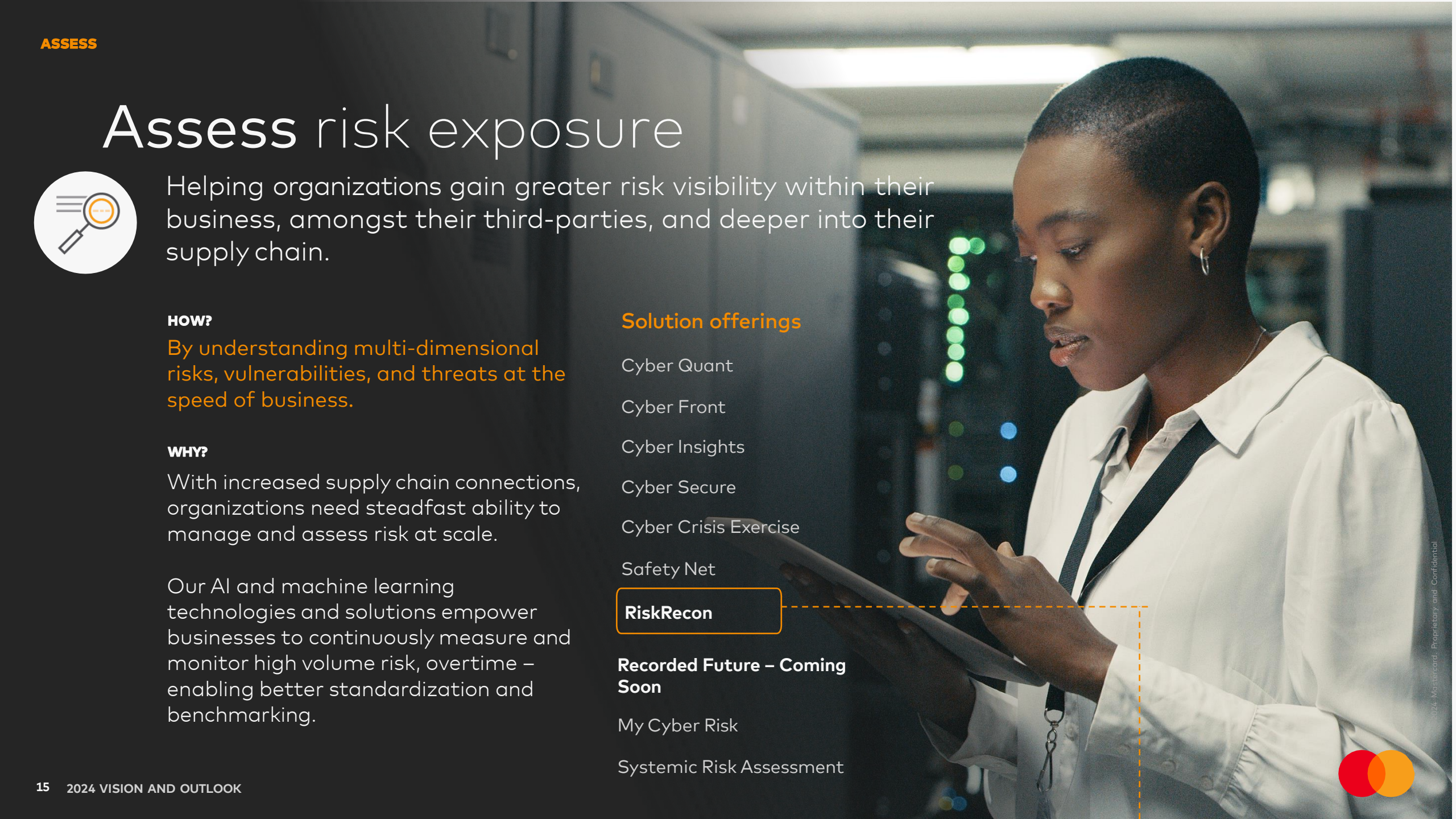
Safety Net

RiskRecon

Recorded Future – Coming Soon

My Cyber Risk

Systemic Risk Assessment



MASTERCARD CYBERSECURITY

One trusted approach

Supported by Mastercard's Cybersecurity Solutions Partner Services

Our portfolio of cyber security solutions provides an **unmatched capability** in providing end-to-end cyber risk visibility to organizations of all sizes, positioning us very **uniquely in the market**

Assess
risk exposure

Understanding multi-dimensional risks, vulnerabilities, and threats at the speed of business

Solution offerings

- **Cyber Quant:** Cybersecurity Maturity & Financial Risk Quantification.
- **Cyber Front:** Breach and Attack Simulation
- **Cyber Insights:** Strategic Threat Intelligence Trends
- **RiskRecon:** Third Party Risk Monitoring

Protect
against attacks

Addressing risks using unique intelligence and multi-layered cloud-based defense technology

Solution offerings

- **Cyber Front:** Breach and Attack Simulation
- **Threat Protection:** Cloud-Based DDoS Protection

Organize
ecosystem trust

Orchestrating continuous improvement of global cyber security and risk

Solution offerings

- **Cyber Crisis Exercise:** Interactive Cyber Crisis Scenario Exercising.

SOLUTION

RiskRecon helps you to effectively assess cyber risk from third-party business relationships

RiskRecon proactively monitors the cyber environment of any entity with an online presence to identify cyber risks and vulnerabilities before they can be exploited.

By effectively assessing cyber risk from third parties, organizations can ensure they do not fall victim to cyber attacks from the risks incurred through their business relationships.

riskrecon by

FEATURES

Pinpoint and prioritize cyber risk from third parties

Aggregated **cyber risk rating** for every third-party service provider and vendor based on the assessment of their cyber environment

AI-driven assessments capabilities streamline the vendor **questionnaire process** to initiate assessments, summarize complex documents, and cross-check compliance across your vendor catalog.

Alerts on issues exceeding risk thresholds along with in-portal viewing and alert management through the **Alert management center**

Downloadable **detailed, summary and executive summary reports** on overall organization cyber risk profile on demand

Benchmarking of third-party service providers and vendors against standardized compliance frameworks and amongst comparable competitors

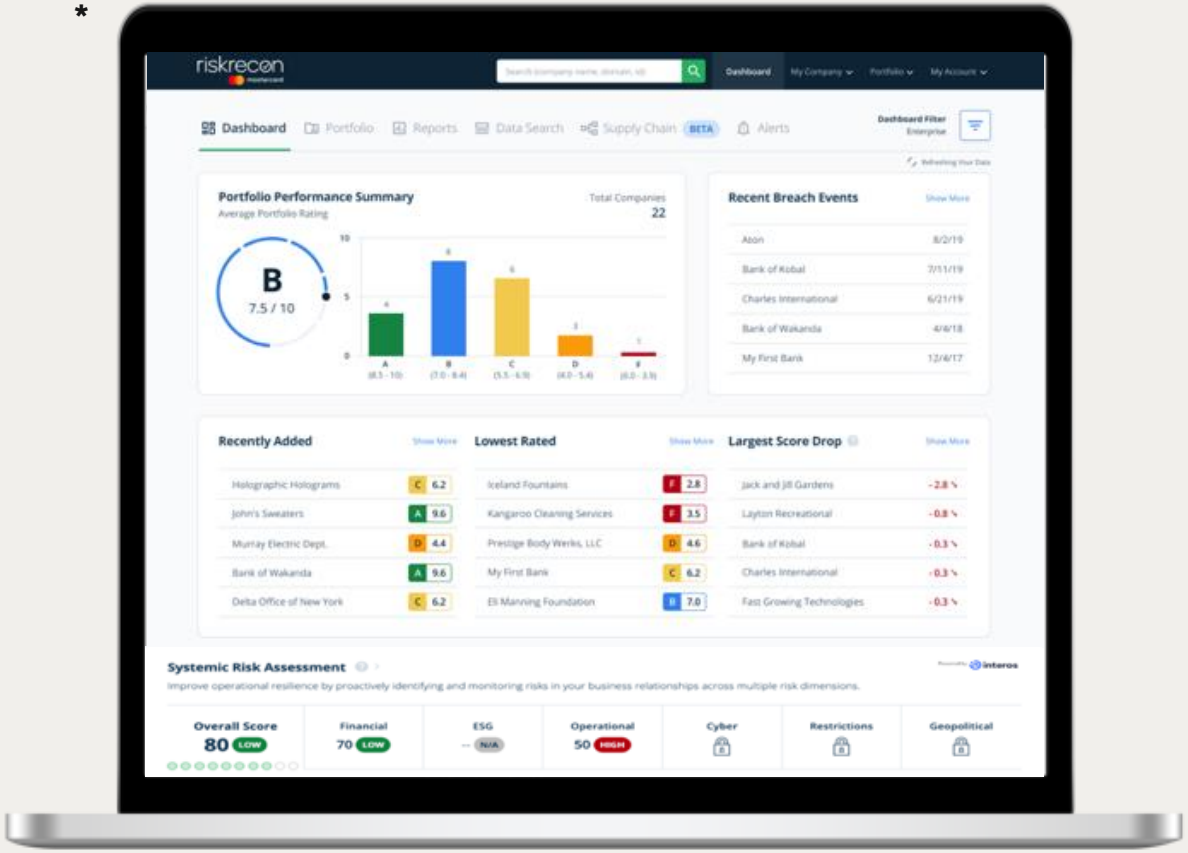
Actionable risk plans are easily shared with third-party service providers and vendors using the collaboration portal

View of organization's cyber risk visibility to their extended supply chain of **fourth-party providers**

Aggregated systemic risk* scores evaluated across all business relationships for **financial, ESG, and operational risk dimensions** via Mastercard SRA

Did you know?
Companies with cyber risk rating of 'F' are **4x** more likely to experience a data loss event according to RiskRecon analysis.

*



*Systemic risk refers to the risk of a cascading failure, caused by linkages within the financial system, resulting in significant business impact.
*For illustrative purposes only

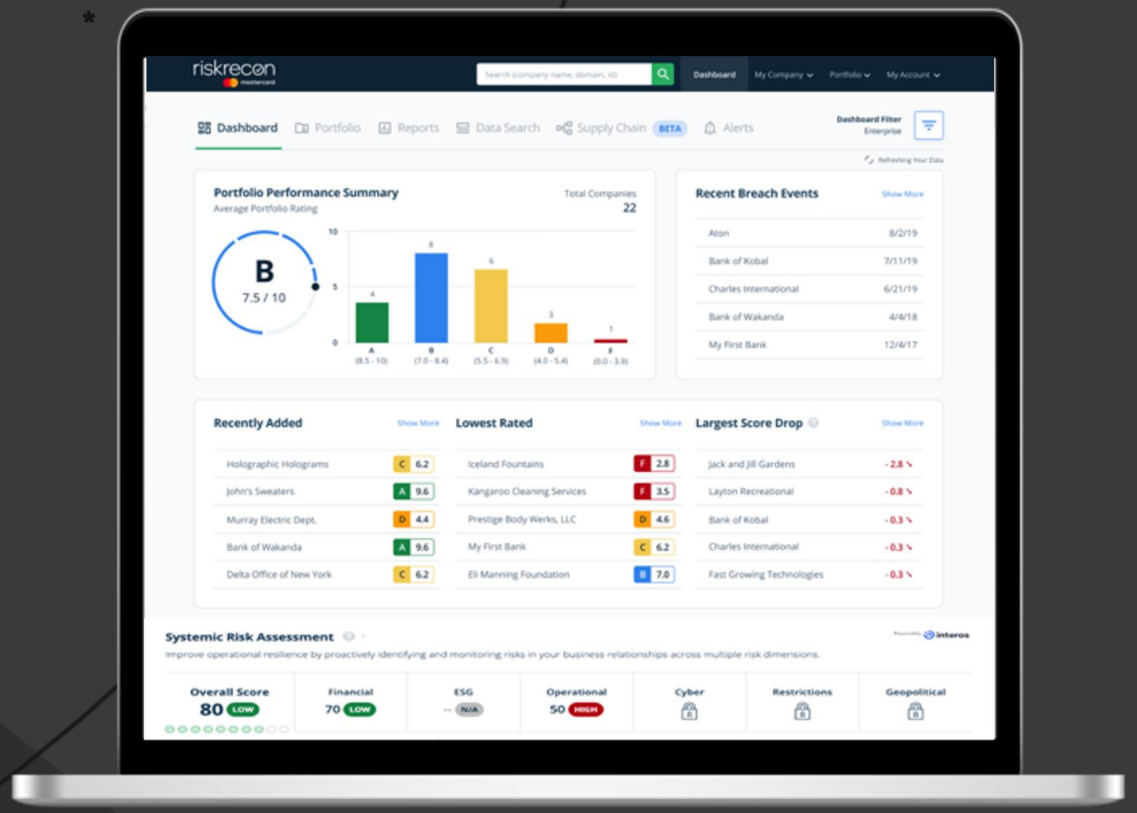
riskrecon by

"How do we stay out of headlines?"

- Don't rely solely on a security questionnaire to assess your vendors
- Utilize a layered approach to ensure you have full visibility into the risks/threats present at any given point in time
- Risks and threats are not static
  - Doing what we have always done doesn't make sense anymore
  - We need to be able to chart a new course when needed

Questions?

Free 30-day trial of RiskRecon by Mastercard:
riskrecon.com/know-your-portfolio



What can you expect from your 30-day access?

- Security ratings for 50 vendors in your ecosystem
- A RiskRecon report of your own organization
- Risk prioritized security findings via RiskRecon's unique Risk Priority Matrix